the input scanner **12**. If no security mark SM has been found, reproduction of the document is permitted. If, on the other hand, a security mark SM is identified, a prevention sub-step S6*b* prevents effective duplication of the document scanned by the input scanner **12**. This is accomplished using one or more suitable prevention operations such as disabling the image output device **16**, not sending output data from the image processing unit **14** to the image output device **16**, embedding or otherwise including a message (such as VOID) in the image data sent to the image output device **16** so that the message is visible in the document reproduction, or by any other suitable method that prevents an effective reproduction of the document scanned by the input scanner **12**.

The invention has been described with reference to preferred embodiments. Modifications and alterations will occur to others upon reading and understanding the preceding specification. It is intended that the invention be construed as including all such modifications and alterations insofar as they fall within the scope of the appended claims or equivalents thereof.

Having thus described the preferred embodiments, what is claimed is:

1. A digital image processing method for preventing unauthorized reproduction of a printed document including a security mark defined in terms of a plurality of actual mark constituents having a select color, select dimensions and arranged in a select pattern relative to each other, said method comprising:

a. scanning said printed document to derive color digital data representing said printed document, said color digital data defined in terms of a plurality of pixels each having a color value;

b. identifying all pixels of said color digital data having a color value representing a color at least approximating said select color of said plurality of actual mark constituents;

c. constructing a binary map of said color digital data defined in terms of "on" and "off" pixels, said "on" pixels corresponding to said identified pixels of said color digital data having color values at least approximating said select color of said plurality of actual mark constituents;

d. using said binary map, identifying potential mark constituents defined by said "on" pixels, said step of identifying potential mark constituents by said "on" pixels comprising:

processing said pixels of said binary map to identify groups of at least one adjacent "on" pixel and identifying each of said groups as a connected component;

comparing dimensions of each connected component to the predefined select dimensions of an actual mark constituent comprising the steps of:

comparing a width of the connected component to minimum and maximum width values of an actual mark constituent;

comparing a height of the connected component to minimum and maximum height values of an actual mark constituent;

only for each connected component having both a width encompassed by said minimum and maximum width values and having a height encompassed by said minimum and maximum height values, comparing the connected component to at least one template, said connected component identified as a potential mark constituent if said connected component matches said at least one template;

e. using said binary map, identifying at least one neighborhood of plural potential mark constituents together defining a potential security mark;

f. identifying said potential security mark as an actual security mark if said potential mark constituents thereof are uniform relative to each other; and

g. preventing effective duplication of said printed document if an actual security mark is identified.

2. The digital image processing method as set forth in claim **1** wherein said step (f) of identifying an actual security mark comprises:

comparing all potential mark constituents of a potential security mark to each other and identifying a potential security mark as an actual security mark if the potential mark constituents defining the potential security mark are uniform relative to each other in terms of at least color and size.

3. A digital image processing method for preventing unauthorized reproduction of a printed document including a security mark defined in terms of a plurality of actual mark constituents having a select color, select dimensions and arranged in a select pattern relative to each other, said method comprising:

a. scanning said printed document to derive color digital data representing said printed document, said color digital data defined in terms of a plurality of pixels each having a color value;

b. identifying all pixels of said color digital data having a color value representing a color at least approximating said select color of said plurality of actual mark constituents;

c. constructing a binary map of said color digital data defined in terms of "on" and "off" pixels, said "on" pixels corresponding to said identified pixels of said color digital data having color values at least approximating said select color of said plurality of actual mark constituents;

d. using said binary map, identifying potential mark constituents defined by said "on" pixels;

e. using said binary map, identifying at least one neighborhood of plural potential mark constituents together defining a potential security mark, said step of identifying at least one neighborhood comprising:

establishing a neighborhood about the potential mark constituent;

counting the number of potential mark constituents located in the neighborhood;

comparing the number of potential mark constituents in the neighborhood to the number of potential mark constituents used to define an actual security mark; and

identifying a neighborhood as a potential security mark only if the number of potential mark constituents therein is equal to or greater than the number of actual mark constituents required to define an actual security mark;

f. identifying said potential security mark as an actual security mark if said potential mark constituents thereof are uniform relative to each other; and

g. preventing effective duplication of said printed document if an actual security mark is identified.

4. The digital image processing method as set forth in claim **3** wherein said neighborhood established about each potential mark constituent has a radius based upon a predefined maximum distance between any two actual mark constituents defining an actual security mark in said printed document.